Submission in Response to NSF CI 2030 Request for Information

DATE AND TIME: 2017-03-23 09:14:07
REFERENCE NO: 191

Author Names & Affiliations

- Alan Blatecky - RTI-International

Contact Email Address (for NSF use only)

(Hidden)

Research Domain, discipline, and sub-discipline

Cyberinfrastructure, computer science, engineering

Title of Submission

Three components required to develop advanced cyberinfrastructure to support Science and Engineering Research

Abstract (maximum ~200 words).

The cyberinfrastructure that will be available to support research in 2030 will be vastly different from what exists today, and will have a number of capabilities that we don't envision today. As Kevin Kelly points out about the future of Artificial Intelligence , in ten years, people will be using AI applications that haven't been invented yet, so it's not too late to start; cyberinfrastructure is in the same boat.

Cyberinfrastructure is being driven by an unusual confluence of technologies, capabilities, and factors that will significantly transform what is done, including what we do and how we do it. Although enormous commercial efforts will be focused on developing new technologies, new business and service opportunities, cyberinfrastructure also provides enormous opportunities for science, research, and education. These factors will combine and coalesce to create an ever evolving cyberinfrasturcture that will impact our entire social structure and ecosystems; personal, community, government, science, business, leisure and education.

The growing importance of cyberinfrastructure to support research and science in 2030 requires NSF to better organize how it will manage and support domain-driven cyberinfrastructure, interoperable cyberinfrastructure, and, cyberinfrastruture research. This includes a regular cadence of financial investments as well as more emphasis upon sustainability.

Question 1 Research Challenge(s) (maximum ~1200 words): Describe current or emerging science or engineering research challenge(s), providing context in terms of recent research activities and standing questions in the field.

Component 1 -- Domain-driven cyberinfrastructure

Since cyberinfrastructure will become ever more important to support research in all scientific domains over the next two decades, it is

essential that NSF supports a focus to develop collaborative and intellectual partnerships among scientific domain teams and cyberinfrastruture teams to embed cyberinfrastructure into specific science challenges from the outset. In these scenarios, development of tools and capabilities will be driven domain researchers to create new approaches to research as well as beginning to address scientific challenges we're not able to address today because of inadequate technologies and data. These new domain-driven tools, approaches, and capabilities, will in turn, be applied to other disciplines, research, and grand challenge problems.

Challenges
• NSF needs to find ways to effectively support joint solicitations and partnered research between Directorates and OACI
• Effective cyberinfrastructure evangelism and advocacy is required to bring new technologies and approaches to the attention of domain scientists; providing a cross community focus for all things involving advanced cyberinfrastructure for science and education; supporting some sort of a cyberinfrastructure "clearinghouse"
• Need to effectively support and address issues associated with building new science communities and partnerships. This will require a focus on pilots, proofs-of-concepts, and incubation, and supporting the development of new social, organizational, and diverse teams including a trained and educated workforce for the next two decades including developing corps of cyberpractitioners.
• Need to encourage and support the development of AI-partnered research to create entirely new ways of doing science. This includes supporting Artificial Intelligence/human symbiotic activities and relationships; deployment of augmented systems and dependencies; complex networks with embedded sensors, HPC/HTC compute, and Artificial Intelligence.
• It is essential to address fundamental issues associated with cyberinfrastructure (cyber-security, re-use of data and software, etc) at the outset when domain-driven projects develop and implement new approaches to science involving cyberinfrastructure; this includes coordinating with other international cyberinfrastructure efforts.

Question 2 Cyberinfrastructure Needed to Address the Research Challenge(s) (maximum ~1200 words): Describe any limitations or absence of existing cyberinfrastructure, and/or specific technical advancements in cyberinfrastructure (e.g. advanced computing, data infrastructure, software infrastructure, applications, networking, cybersecurity), that must be addressed to accomplish the identified research challenge(s).

Component 2 -- Cyberinfrastructure integration and interoperability

One of the biggest challenges in the development and support of cyberinfrastructure over the next two decades will be to find ways to effectively build and deploy integrated cyberinfrastructure that supports sharing and interoperability. What makes this very challenging, is that it is not possible to develop a common universal cyberinfrastructure architecture that will meet the needs of research and education. Cyberinfrastructure can only be effectively deployed when it is developed to address specific implementations and applications. There are numerous examples of the failure of a "build it and they will come" approach that has been used in the past. This means that the impetus for development must come from domains and researchers who are doing research or trying to solve one or more problems.

This approach in turn creates a range of problems that need to be addressed, including reinvention, duplication, redundancy, lack of scale, lack of interoperability and little incentive to work on integration or sharing of resources and capabilities as these efforts do not directly accrue to or directly benefit the research being done. Perhaps even worse, if interoperability and the ability to share is not considered to be part of an end product (data, tools, capabilities) in one field, it cannot be used to support research in other fields, and the resulting negative impact on scientific discovery and innovation will be huge.

Challenges
• Need to incentivize and encourage research awardees to ensure that any project efforts that include cyberinfrastructure development, also focus on making sure their products and outputs interoperate and integrate with other existing cyberinfrastructure technologies, approaches and tools. At the same time, it will be essential to recognize the appropriate balance of effort between basic development versus delivery of publicly available common interfaces or APIs.

• It is essential to address fundamental issues associated with interoperability, cyber-security, tool re-use, software, networking, generation and re-use of data should be addressed at the outset when projects are conceived and funded.

• The importance of integration and interoperability of cyberinfrastructure suggests that projects should include objectives and processes to foster interoperability from the start of an award. This will require more use of developers who have familiarity and knowledge of how to

develop open APIs and support community standards.

• Successful integration depends upon effective multidisciplinary teams working with heterogeneous cybersystems (security, networking, data, HPC, etc). Because emerging cybersystems both leverage and exploit new technologies and approaches, effective teaming between cyberinfrastructure experts and domain experts is required.

• Successful integration also depends on having some captive cyberinfrastructure instruments and or cybersystems in place to support both science as well as development. Effective data interoperability testing and development can requires the use of a real data repository that has data analytic tools and a domain independent infrastructure.

• Issues of scaling, integration, and interoperability, along with some sort of light coordination across projects will also become ever more important to reduce redundancy and needless replication. Even more important than not letting each project award develop their own unique cyberinfrastructure approach and silo because of cost reasons, the inability to share tools and approach will have a disastrous impact on new science and discovery as projects will not be able to leverage or reuse capabilities or result from one project to another. One huge challenge facing NSF will be how to develop effective ways to encourage integration and support some type of coordination across both national and international boundaries, especially connectivity and capacity.

Question 3 Other considerations (maximum ~1200 words, optional): Any other relevant aspects, such as organization, process, learning and workforce development, access, and sustainability, that need to be addressed; or any other issues that NSF should consider.

Component 3- cyberinfrastructure research

Cyberinfrastructure is being driven by an unusual confluence of technologies, capabilities, and factors that will significantly transform what is done, including what we do and how we do it. Although enormous efforts will be focused on developing new technologies, new business and service opportunities, including personal devices and new applications, cyberinfrastructure will also provide enormous opportunities for science, research, and education. These factors include the following:
• On-going relentless changes from Moore's Law and other advances will continue to affect all things digital and compute based; for the next decade, things will continue to get cheaper, faster and more powerful, to the point that many devices will be disposable or throwaway. And, when things become perceived as a "free resource", they will be used in totally new ways to address new functionalities. In this environment, substitution effects means that the function and purpose of a particular device may be used for something totally different than originally intended.
• The Internet Of Things will create vast new capabilities, technologies, and devices across the entire spectrum of human activities and around the globe; powerful sensors will be embedded into everything thing from toys and appliances to cars, bridges, factories (anything that moves or is used) and networks. The intersection of IOT and big data analytics and other initiatives such as smart cities, smart agriculture, smart health, along with issues of scale, will transform what can be done providing entirely new types of science and research.
• Specific emerging technologies like 5G will provide a level and speed of interconnectedness that is unprecedented. Moreover, because it is wireless, geography and location will matter even less in the future, and will generate new applications and opportunities. New capabilities, such as cognitive radios and picocells coupled with reducing the "final mile" access connections, will create totally new networks and capabilities and dramatically reduce barriers to entry.
• The generation and accumulation of data will continue to rise unabated and will continue to be fueled as the cost-per-bit to generate and collect data continues to drop dramatically. The growth in data will be driven both by market forces (new devices, services, applications), as well as by a curiosity to know more. Our innate desire to have more control over what happens in our lives will mean that there will be a new urgency and capability for individual agency and community use. Our notions of privacy, security, acceptable use, and identification, will significantly morph as digital personas become the norm.
• Over the next decade, Artificial Intelligence will be part and parcel of a tremendous range of devices, activities and applications, but more significantly, it will be coupled with technology advances and human endeavors in ways that enables people to do things that people have never been able to do before. AI will drive new discoveries, as well as introduce new fields of science and ways to do research. AI will also drive the selection of hardware as well as the design in hardware as it becomes instantiated into products and capabilities (AI won't just be mapped onto existing platforms, but AI will be involved in the design of the platforms up front)

These factors will combine and coalesce to create an ever evolving cyberinfrasturcture that will impact our entire social structure and ecosystems; personal, community, government, science, business, leisure and education.

Although the bulk of cyberinfrastructure technologies and capabilities over the next two decades will be driven by the confluence of Moore's Law, the Internet Of Things, 5G, Artificial Intelligence, HPC, and so forth, business and industry will do the lion's share of the development as they seek out new opportunities and lines of business. That being said, it is essential that NSF play a central role in adapting these emerging technologies and capabilities in service to science, and also in helping to push and fund cyberinfrastructure research boundaries to do new science. This will involve a wide range of areas, from supporting basic foundational cyberinfrastructure research, to developing pilots and test beds, promoting structured workshops to address emerging capabilities and developing new applications.

Challenges
• While the confluence of factors will continue to drive the development of cyberinfrastructure in general, NSF should focus on developing those components or capabilities of cyberinfrastructure that specifically support engineering and research. This will include not only the domain-driven cyberinfrastructure listed above, but will include basic foundational cyberinfrastructure research leading to new capabilities such as new compute architectures and infrastructure; challenges associated with embedding Artificial Intelligence into the conduct of science; new network architectures as fiber and wireless capabilities eliminate issues of geographic location; proliferation of IOT devices that can be used or modified to support science; coordination with other international efforts.

• A second challenge of cyberinfrastructure research should be on integrating various technologies, disparate components, or capabilities to work together to support scientific discovery. This would include the development of pilots and proofs-of-concept to test or validate usefulness, especially for those approaches that create new types of ecosystems (embedded AI, sensors, etc) that explore science. Other efforts would include exploring new cyberinfrastructure environments and capabilities such as "cloudettes" (personal cloud computing based on extra compute capacity of deployed devices), establishment of test beds that support integration and helping to create the multidisciplinary workforce to support science over the next 2 decades.

• A third challenge is to address research issues associated with a "human-in-the-loop" cyberinfrastructure. This includes a holistic approach to the cyberinfrastructure environment as identification and authentication begins to extend to genomics and DNA and where real-time awareness and geo-tracking raises new levels of physical insecurity. It also goes far beyond human interfaces and explores AI/symbiotic interfaces as devices and intelligence become handmaidens of human efforts, where automatic awareness, assistance capabilities, and bots will do things without our conscious or proactive involvement. This will also include the establishment and support of new "tribes" or research communications who conduct science with a set of tools and at a scale almost unimaginable today.

• The explosive growth and evolution of cyberinfrastructure over the next two decades will stress the ability of the science and engineering communities to effectively use the developments for science, and yet it will be critical for NSF to continue to provide leadership on what cyberinfrastructure research should be supported and pursued. This is turn will mean that NSF should be more aggressive about providing and supporting a process to not only track the growth and evolution of cyberinfrastructure, but also more fully engage the community in state-of-the-art developments.